UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/713,896	01/31/2003	Dan Revital	7251-94634	8262

24628 7590 09/11/2007

WELSH & KATZ, LTD
120 S RIVERSIDE PLAZA
22ND FLOOR
CHICAGO, IL 60606

EXAMINER	
DOAN, TRANG T	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
09/11/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/713,896	REVITAL ET AL.	
	Examiner	Art Unit	
	Trang Doan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 April 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50 and 83-117* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50 and 83-117* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the amendment filed on 04/23/2007.

2. Claims 1-50 and 83-117 are pending for consideration.

Claim Objections

3. Regarding claims 2, 5, 13-14, 16-18, 22, 40-42, 46-48, 84-85, 90, 101-103, 107 and 115-116, the Applicant requires to spell out all of the abbreviated symbols, e.g., ECM, EMM, VEMM and VECM. Appropriate correction is required.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-3, 29-30, 32-39, 43-47 and 49-50 are rejected under 35 U.S.C. 102(e) as being anticipated by Akaue et al. (US 2002/0116622) (hereinafter Akaue).

6. Regarding claim 1, a security server (Akaue: see figure 1, ref. 10, a content data distributing); a recipient module (Akaue: see figure 1, ref. 20, data processing means receive and decode received contents data and contents keys from content data distributing); and a secure communication channel for supporting communication

between said security server and said recipient module, wherein, in a first mode of operation, the recipient module receives a first key in a multiple key hierarchy via said secure channel, and in a second mode of operation, the recipient module receives the protected content and an encrypted key, said encrypted key being a second key in said multiple key hierarchy, said recipient module being operative to utilize the first key to decrypt the encrypted key to form a decrypted key, said recipient module only being capable of accessing the protected content with said decrypted key (Akaue: see figures (3, 9-10, 30, 33 and 46), Abstract section and paragraphs 0141, 0145 and 0520-0523, enabling key block-1 (EKB-1) is used for generating a contents key (Kcon-1) ciphered from a content data 1).

7. Regarding claim 2, Akaue further discloses wherein said first key is contained in a VEMM, said VEMM further comprising an access criteria reference for determining whether said recipient module is entitled to access the protected content and said VEMM being prepared by said security server (Akaue: see paragraphs 0142-0143).

8. Regarding claim 3, Akaue further discloses wherein said access criteria reference for each item of protected content is associated with a separate access key (Akaue: paragraph 0014).

9. Regarding claim 29, Akaue discloses (a) a remote renewable security element for encrypting a plurality of keys in a multiple key hierarchy (Akaue: see figures 3, 7, 13, 28 and 44-46); and (b) a recipient module for receiving the protected content and said plurality of encrypted keys, said recipient module comprising a secret for decrypting at least one encrypted key to form a first decrypted key, said first decrypted key being

required to decrypt at least one additional key in said multiple key hierarchy, wherein said recipient module is only capable of accessing the protected content with said at least one additional decrypted key in said multiple key hierarchy (Akaue: see figures 28, 43 and paragraphs 0117 and 0141-0142).

10. Regarding claims 30, Akaue further discloses wherein said first encrypted key is only capable of being decrypted according to said secret (Akaue: see figure 30).

11. Regarding claim 32, Akaue further discloses wherein said secret is permanently stored on said at least one permanent read-only storage medium during manufacture of said recipient module (Akaue: paragraphs 0005 and 0174).

12. Regarding claim 33, Akaue further discloses wherein said recipient module comprises at least one generic chip, said at least one generic chip comprising said at least one permanent read-only storage medium for storing said secret (Akaue: paragraphs 0005 and 0174).

13. Regarding claim 34, this claim has limitations that is similar to those of claim 24, thus it is rejected with the same rationale applied against claim 24 below.

14. Regarding claim 35, Akaue further discloses wherein at least one of said keys in said multiple key hierarchy at said remote renewable security element is capable of being renewed (Akaue: see figures 3 and 11 and paragraph 0115).

15. Regarding claim 36, Akaue further discloses wherein said remote renewable security element comprises at least one encryption mechanism (Akaue: see figure 4).

16. Regarding claim 37, this claim has limitations that is similar to those of claim 11, thus it is rejected with the same rationale applied against claim 11 below.

17. Regarding claim 38, this claim has limitations that is similar to those of claim 12, thus it is rejected with the same rationale applied against claim 12 below.

18. Regarding claim 39, this claim has limitations that is similar to those of claim 2, 3 and 5, thus it is rejected with the same rationale applied against claims 2, 3 and 5 below.

19. Regarding claim 43, this claim has limitations that is similar to those of claim 27, thus it is rejected with the same rationale applied against claim 27 below.

20. Regarding claim 44, this claim has limitations that is similar to those of claim 5 and 19, thus it is rejected with the same rationale applied against claim 5 and 19 below.

21. Regarding claim 45, this claim has limitations that is similar to those of claim 14, thus it is rejected with the same rationale applied against claim 14 above.

22. Regarding claim 46, this claim has limitations that is similar to those of claim 14, thus it is rejected with the same rationale applied against claim 14 above.

23. Regarding claim 47, this claim has limitations that is similar to those of claim 15, thus it is rejected with the same rationale applied against claim 15 above.

24. Regarding claim 49, this claim has limitations that is similar to those of claim 28, thus it is rejected with the same rationale applied against claim 28 above.

25. Regarding claim 50, Akaue further discloses wherein each access criteria reference is associated with a different access key (Akaue: see figures 3, 11 and 13).

Claim Rejections - 35 USC § 103

26. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

27. Claims 4-28, 31, 40-42, 48 and 83-117 are rejected under 35 U.S.C. 103(a) as being unpatentable over Akaue in view of Wasilewski et al (US 6971008) (hereinafter Wasilewski).

28. Regarding claim 4, Akaue does not explicitly disclose in detail wherein said encrypted key further comprises an encrypted control word. However, Wasilewki discloses wherein said encrypted key further comprises an encrypted control word (Wasilewki: see figure 2B and column 7 lines 15-35). Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to combine the teaching of Wasilewki within the system of Akaue because Wasilewki discloses providing the encrypted control word to the recipient module that requires access restrictions which are both more secure and more flexible than those in conventional systems (Wasilewki: column 3 lines 1-3).

29. Regarding claim 5, Akaue does not explicitly disclose wherein said encrypted control word is contained in a VECM, said VECM further comprising an access criteria reference for identifying said first key for decrypting said encrypted control word by said recipient module and said VECM being prepared by said security server. However, Wasilewki discloses wherein said encrypted control word is contained in a VECM, said

VECM further comprising an access criteria reference for identifying said first key for decrypting said encrypted control word by said recipient module and said VECM being prepared by said security server (Wasilewki: see figure 2B and column 7 lines 15-35). Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to combine the teaching of Wasilewki within the system of Akaue because Wasilewki discloses providing the encrypted control word to the recipient module that requires access restrictions which are both more secure and more flexible than those in conventional systems (Wasilewki: column 3 lines 1-3).

30. Regarding claim 6, Akaue in view of Wasilewki further discloses wherein said secure communication channel further comprises a subscriber key, such that said first key is encrypted with said subscriber key for being transmitted to said recipient module, and such that said recipient module is capable of decrypting said subscriber key (see figure 9).

31. Regarding claim 7, Akaue in view of Wasilewki further discloses wherein said recipient module further comprises a secret, said secret being required for decrypting said subscriber key, and said secret comprising a part of said secure communication channel (Akaue: see figure 43 and paragraph 0174, including data necessary for the authentication process).

32. Regarding claim 8, Akaue in view of Wasilewki further discloses wherein said recipient module comprises at least one permanent read-only storage medium for storing said secret (Akaue: paragraphs 0005 and 0174).

33. Regarding claim 9, Akaue in view of Wasilewki further discloses wherein said secret is permanently stored on said at least one permanent read-only storage medium during manufacture of said recipient module (Akaue: paragraphs 0005 and 0174).

34. Regarding claim 10, this claim has limitations that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

35. Regarding claim 11, Akaue in view of Wasilewki further discloses wherein said security server receives said subscriber key encrypted with said secret and an unencrypted subscriber key, but wherein said security server does not receive said secret (Akaue: see figure 15).

36. Regarding claim 12, Akaue in view of Wasilewki further discloses a head-end for transmitting the protected content (Akaue: paragraph 0100).

37. Regarding claims 13 and 40, Akaue does not explicitly disclose wherein said head-end sends a EMM to said security server, for providing said access criteria reference to said security server. However, Wasilewki discloses wherein said head-end sends a EMM to said security server, for providing said access criteria reference to said security server (Wasilewki: see figure 1 and column 5 lines 3-20). Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to combine the teaching of Wasilewki within the system of Akaue because Wasilewki discloses the EMM that is needed to control not only who can access a given instance of a service, but also what entities can offer services to a given receiver (Wasilewki: column 6 lines 20-23).

38. Regarding claim 14, Akaue does not explicitly disclose wherein said head-end sends at least information for generating said control word to said security server in an ECM. However, Wasilewki discloses wherein said head-end sends at least information for generating said control word to said security server in an ECM (Wasilewki: see figure 2A). Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to combine the teaching of Wasilewki within the system of Akaue because Wasilewki discloses the ECM distributed by the head-end to the recipient module that is needed to control not only who can access a given instance of a service, but also what entities can offer services to a given receiver (Wasilewki: column 6 lines 20-23).

39. Regarding claim 15, Akaue does not explicitly disclose wherein said head-end also sends said ECM to said recipient module. However, Wasilewki discloses wherein said head-end also sends said ECM to said recipient module (see figure 1). Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to combine the teaching of Wasilewki within the system of Akaue because Wasilewki discloses the ECM distributed by the head-end to the recipient module that is needed to control not only who can access a given instance of a service, but also what entities can offer services to a given receiver (Wasilewki: column 6 lines 20-23).

40. Regarding claim 16, Akaue in view of Wasilewki further discloses wherein a different VEMM is transmitted periodically (Akaue: paragraphs 0030 and 0114-0115).

41. Regarding claim 17, this claim has limitations that is similar to those of claim 16, thus it is rejected with the same rationale applied against claim 16 above.

42. Regarding claim 18, Akaue in view of Wasilewki further discloses comprising a plurality of recipient modules, wherein said VEMM is unicast to each of a subset of said plurality of recipient modules (Akaue: see figure 3 and paragraphs 0017, 0022 and 0111).

43. Regarding claim 19, Akaue does not explicitly disclose a remote renewable security element for storing said subscriber key and for providing said encrypted first key and said encrypted control word to said security server. However, Wasilewki discloses a remote renewable security element for storing said subscriber key and for providing said encrypted first key and said encrypted control word to said security server (Wasilewki: column 31 lines 28-47). Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to combine the teaching of Wasilewki within the system of Akaue because Wasilewki discloses the remote renewable security element that is needed to control not only who can access a given instance of a service, but also what entities can offer services to a given receiver (Wasilewki: column 6 lines 20-23).

44. Regarding claim 20, this claim has limitations that is similar to those of claim 19, thus it is rejected with the same rationale applied against claim 19 above.

45. Regarding claim 21, this claim has limitations that is similar to those of claim 19, thus it is rejected with the same rationale applied against claim 19 above.

46. Regarding claim 22, Akaue does not explicitly disclose wherein said software component determines one or more entitlements for permitting said VEMM to be generated for said recipient module. However, Wasilewki discloses wherein said

software component determines one or more entitlements for permitting said VEMM to be generated for said recipient module (Wasilewki: column 4 lines 24-46 and column 5 lines 3-21). Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to combine the teaching of Wasilewki within the system of Akaue because Wasilewki discloses the entitlement control message that is needed to control not only who can access a given instance of a service, but also what entities can offer services to a given receiver (Wasilewki: column 6 lines 20-23).

47. Regarding claim 23, this claim has limitations that is similar to those of claim 4, thus it is rejected with the same rationale applied against claim 4 above.

48. Regarding claim 24, Akaue in view of Wasilewki further discloses a plurality of said remote renewable security elements, and further comprising a broadcaster of the protected content for controlling said plurality of said remote renewable security elements (Akaue: figures, 5, 7, 9 and 10).

49. Regarding claim 25, Akaue in view of Wasilewki further discloses wherein a plurality of said remote renewable security elements is controlled by said security server (Akaue: see figure 43).

50. Regarding claim 26, Akaue in view of Wasilewki further discloses wherein said security server and said plurality of said remote renewable security elements share a server key for at least decrypting at least said access key (Akaue: see figures 3 and 44-46).

51. Regarding claim 27, Akaue in view of Wasilewki further discloses wherein said security server generates said access key in an encrypted form as an encrypted access

key, and wherein said remote renewable security element decrypts said encrypted access key to form said access key according to said server key (Akaue: see figures (3, 9-10, 30, 33 and 46), Abstract section and paragraphs 0141, 0145 and 0520-0523, enabling key block-1 (EKB-1) is used for generating a contents key (Kcon-1) ciphered from a content data 1).

52. Regarding claim 28, Akaue in view of Wasilewki further discloses wherein said recipient module comprises a set-top box (Akaue: paragraph 0100).

53. Regarding claim 41, this claim has limitations that is similar to those of claims 14 and 15, thus it is rejected with the same rationale applied against claims 14 and 15 above.

54. Regarding claim 42, this claim has limitations that is similar to those of claim 16, thus it is rejected with the same rationale applied against claim 16 above.

55. Regarding claim 48, Akaue does not explicitly disclose a set-top box for receiving the protected content, said set-top box comprising a smart card located at said set-top box, said set-top box receiving said ECM and said EMM from said head-end if said set-top box is authorized to access the protected content, such that said set-top box is not required to be in communication with said security server. However, Wasilewki discloses a set-top box for receiving the protected content, said set-top box comprising a smart card located at said set-top box, said set-top box receiving said ECM and said EMM from said head-end if said set-top box is authorized to access the protected content, such that said set-top box is not required to be in communication with said security server (Wasilewki: column 4 lines 24-46, column 5 lines 3-21 and column 21

lines 25-38). Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to combine the teaching of Wasilewki within the system of Akaue because Wasilewki discloses the entitlement control message that is needed to control not only who can access a given instance of a service, but also what entities can offer services to a given receiver (Wasilewki: column 6 lines 20-23).

56. Regarding claim 83, Akaue discloses a head-end operative to send entitlement information controlling access to the protected content; a security server (Akaue: see figure 1); a plurality of recipient modules (Akaue: see figure 1); and a secure communication channel for supporting communication between said security server and at least one of said plurality of recipient modules (Akaue: see Abstract section), wherein the head-end sends the entitlement information both to the security server and to at least some of the plurality of recipient modules; and said plurality of recipient modules comprises: a first plurality of security-element recipient modules; and a second plurality of non-security-element recipient modules, the first plurality of recipient modules differing from said second plurality of recipient modules in that each of the first plurality of security-element recipient modules includes a renewable security element operative to process the entitlement information received from the head-end and produce therefrom a key for accessing the protected content, and in a first mode of operation, at least one of the non-security-element recipient modules receives a first key in a multiple key hierarchy via said secure communication channel, and in a second mode of operation, said at least one of the non-security- element recipient modules receives the protected content and an encrypted key, said encrypted key being a second key in said

multiple key hierarchy, said at least one of the non-security-element recipient modules being operative to utilize the first key to decrypt the encrypted key to form a decrypted key, said at least one of the non-security-element recipient modules only being capable of accessing the protected content with said decrypted key, and said first key and said second key are prepared by said security server based, at least in part, on the entitlement information sent by the head-end (Akaue: see paragraphs 0014, 0115-0117, 0153-0154, 0141, 0145 and 0520-0523, enabling key block-1 (EKB-1) is used for generating a contents key (Kcon-1) ciphered from a content data 10617).

Akaue does not disclose the head-end sends the entitlement information to the server and the recipient modules. However, Wasilewki discloses the head-end sends the entitlement information to the server and the recipient modules (Wasilewki: column 4 lines 24-46 and column 5 lines 3-21). Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to combine the teaching of Wasilewki within the system of Akaue because Wasilewki discloses the entitlement control message that is needed to control not only who can access a given instance of a service, but also what entities can offer services to a given receiver (Wasilewki: column 6 lines 20-23).

57. Regarding claim 84, this claim has limitations that is similar to those of claim 83 and 39, thus it is rejected with the same rationale applied against claims 83 and 39 above.

58. Regarding claim 85, Akaue in view of Wasilewki further discloses wherein said VEMM is sent upon request by said at least one of the non-security-element recipient modules (Akaue: paragraph 0613).

59. Regarding claim 86, Akaue in view of Wasilewki further discloses wherein said request includes an access criteria reference (paragraph 0373).

60. Regarding claim 87, Akaue does not disclose wherein said request is initiated in response to an impulse pay per view (IPPV) request by a user. However, Wasilewki discloses wherein said request is initiated in response to an impulse pay per view (IPPV) request by a user (Wasilewki: column 12 lines 50-61). Therefore, it would have been obvious to one ordinary skill in the art at the time the invention was made to combine the teaching of Wasilewki within the system of Akaue because Wasilewki discloses the impulse pay per view (IPPV) request by a user that is needed to control not only who can access a given instance of a service, but also what entities can offer services to a given receiver (Wasilewki: column 6 lines 20-23).

61. Regarding claim 88, this claim has limitations that is similar to those of claim 3, thus it is rejected with the same rationale applied against claim 3 above.

62. Regarding claim 89, this claim has limitations that is similar to those of claim 4, thus it is rejected with the same rationale applied against claim 4 above.

63. Regarding claim 90, this claim has limitations that is similar to those of claim 5, thus it is rejected with the same rationale applied against claim 5 above.

64. Regarding claim 91, this claim has limitations that is similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

65. Regarding claim 92, this claim has limitations that is similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

66. Regarding claim 93, this claim has limitations that is similar to those of claim 7, thus it is rejected with the same rationale applied against claim 7 above.

67. Regarding claim 94, this claim has limitations that is similar to those of claim 8, thus it is rejected with the same rationale applied against claim 8 above.

68. Regarding claim 95, this claim has limitations that is similar to those of claim 9, thus it is rejected with the same rationale applied against claim 9 above.

69. Regarding claim 96, this claim has limitations that is similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

70. Regarding claim 97, this claim has limitations that is similar to those of claim 11, thus it is rejected with the same rationale applied against claim 11 above.

71. Regarding claim 98, this claim has limitations that is similar to those of claim 13, thus it is rejected with the same rationale applied against claim 13 above.

72. Regarding claim 99, this claim has limitations that is similar to those of claim 14, thus it is rejected with the same rationale applied against claim 14 above.

73. Regarding claim 100, this claim has limitations that is similar to those of claim 15, thus it is rejected with the same rationale applied against claim 15 above.

74. Regarding claim 101, this claim has limitations that is similar to those of claim 16, thus it is rejected with the same rationale applied against claim 16 above.

75. Regarding claim 102, this claim has limitations that is similar to those of claim 17, thus it is rejected with the same rationale applied against claim 17 above.

76. Regarding claim 103, this claim has limitations that is similar to those of claim 18, thus it is rejected with the same rationale applied against claim 18 above.

77. Regarding claim 104, this claim has limitations that is similar to those of claim 19, thus it is rejected with the same rationale applied against claim 19 above.

78. Regarding claim 105, this claim has limitations that is similar to those of claim 20, thus it is rejected with the same rationale applied against claim 20 above.

79. Regarding claim 106, this claim has limitations that is similar to those of claim 21, thus it is rejected with the same rationale applied against claim 21 above.

80. Regarding claim 107, this claim has limitations that is similar to those of claim 22, thus it is rejected with the same rationale applied against claim 22 above.

81. Regarding claim 108, this claim has limitations that is similar to those of claim 23, thus it is rejected with the same rationale applied against claim 23 above.

82. Regarding claim 109, this claim has limitations that is similar to those of claim 24, thus it is rejected with the same rationale applied against claim 24 above.

83. Regarding claim 110, this claim has limitations that is similar to those of claim 25, thus it is rejected with the same rationale applied against claim 25 above.

84. Regarding claim 111, this claim has limitations that is similar to those of claim 26, thus it is rejected with the same rationale applied against claim 26 above.

85. Regarding claim 112, this claim has limitations that is similar to those of claim 27, thus it is rejected with the same rationale applied against claim 27 above.

86. Regarding claim 113, this claim has limitations that is similar to those of claim 28, thus it is rejected with the same rationale applied against claim 28 above.

87. Regarding claim 114, Akaue in view Wasilewki further discloses wherein at least one of said security server and said secure communication channel is implemented with redundant components (Akaue: see Abstract section and figure 1).

88. Regarding claim 115, this claim has limitations that is similar to those of claims 40-48 and 83, thus it is rejected with the same rationale applied against claims 40-48 and 83 above.

89. Regarding claim 116, this claim has limitations that is similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

90. Regarding claim 117, this claim has limitations that is similar to those of claim 48, thus it is rejected with the same rationale applied against claim 48 above.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Trang Doan whose telephone number is (571) 272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Trang Doan
Examiner
Art Unit 2131

T.D.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100